REMARKS

In response to the Office Action mailed October 26, 2006, Applicants respectfully request reconsideration. To further the prosecution of this Application, Applicants submit the following remarks, have canceled claims and have added new claims. The claims as now presented are believed to be in allowable condition.

Claims 1-38 were pending in this Application. By this Amendment, claims 2-4, 6, 8-9, 18-20, 23, and 33-35 have been canceled. Applicants expressly reserve the right to prosecute at least some of the canceled claims and similar claims in one or more related Applications. Claims 39-42 have been added. Accordingly, claims 1, 5, 7, 10-17, 21-22, 24-32, and 36-42 are now pending in this Application. Claims 1, 7, 12, 14, 16, 21, 26, 31, 36, 37, and 38 are independent claims.

Rejections under §102 and §103

Claims 1, 4-5, 7, and 9-11 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application No. 2004/0085445 (Park). Claims 14-15 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 7,120,252 (Jones, et al.). Claims 16, 21-25, 31, and 37-38 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application No. 2003/0226023 (Peters). Claims 26, 28-30, and 36 were rejected under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 6,397,334 (Chainer, et al.). Claims 12-13 were rejected under 35 U.S.C. §103(a) as being unpatentable over Chainer in view of U.S. Patent No. 6,870,929 (Greene). Claims 17 and 32 were rejected under 35 U.S.C. §103(a) as being unpatentable over Peters in view of U.S. Patent No. 6,907,123 (Schier). Claim 27 was rejected under 35 U.S.C. §103(a) as being unpatentable over Chainer in view of Schier. Claim 35 was rejected under 35 U.S.C. §103(a) as being unpatentable over Peters in view of Chainer.

Applicants respectfully traverse each of these rejections and request reconsideration. The claims are in allowable condition.

Park discloses a video security system and a method for its operation (Abstract). The system includes a digital camera 100, transmission means 200, a receiving unit 300, a monitor 500, and a warning device 400 (Paragraph 0068). A DSP 120 within the digital camera 100 inserts a series of cumulative time stamp data into blanking intervals of digital video signals output by the camera 100 (Paragraph 0069). If the time stamps are incorrect, a microprocessor 330 on the receiving unit 300 will generate a warning through the warning device 400 (Paragraph 0070).

Peters teaches a technique for deterring theft of media recording devices (Abstract). A media file recorded by a recording device is encrypted, so that it cannot be properly played back without a cryptographic key supplied to the owner of the device (Paragraph 0023). Because asymmetric public key encryption is more secure but also more complex (and therefore slower) than symmetric shared key encryption, a symmetric key may be used to encrypt the media files while the symmetric key is encrypted using public key encryption. (Paragraph 0031). In order to aid a customer who has lost his or her key to a device, a manufacturer may provide a key escrow service to give a customer the key upon presentation of some proof of ownership of the device (Paragraph 0043).

Jones teaches a system and method for protecting video content with cryptography in a legacy system (Abstract). The system intercepts video content 11 being sent to a transportable storage medium (Col. 2, lines 51-54). Individual frames of the intercepted video content 11 are cryptographically hashed, and the resulting cryptographic hash 128 is encrypted with an encryption key 130 to form a digital signature 131 (Col. 9, lines 50-57). Both the video content 11 and the digital signature 131 are stored on a videotape 48. Upon playback of the videotape 48, the system decrypts the digital signature141 to generate a cryptographic hash 144 (Col.9, line 63 through Col. 10, line 4). The system also

cryptographically re-hashes the video content 11 to form a new cryptographic hash 147 (Col. 10, lines 4-6). If the decrypted hash 141 and the new hash 147 match, then the system is able to verify the authenticity of the video (Col.9, line 63 through Col. 10, line 9).

Chainer discloses a system and method for authenticating an image of an object (Abstract). An object 102 contains one or more tags 101, such as RFID tags, which are not functionally removable from the object 102 (Col. 3, line 63 through Col. 4, line 8). A tag reader 103 (such as an RFID tag reader) reads the RFID tags 101 as a coupled camera system 104 records an image of the object 102 (Col. 4, lines 27-36). A composite generator 105 combines the image and the sensed RFID results to encode the tag ID information together with a hash of the image (Col. 4, lines 37-48). This encoded data may be encrypted for further security (Col. 5, lines 43-54). In addition, other measuring devices 400 may record additional properties of an object 406 in order to provide additional information with which to identify an object (Col. 6, lines 17-38). In addition, a zoom lens 108 may be used to take multiple pictures of an object 102 with different settings (Col. 6, lines 39-45).

Claims 1 and 4-5

Independent claim 1 has been amended to include all the limitations previously found in canceled dependent claim 4. Claim 1, as amended, recites a method for obtaining video data. The method includes (a) providing a control signal to a video data acquisition system, (b) receiving an output signal from the data acquisition system in response to providing the control signal, the output signal including video data captured by the video data acquisition system; and (c) verifying an authenticity of the video data from the data acquisition system by checking that the received output signal includes modifications according to the control signal. Providing a control signal includes providing a control signal that includes a command to overlay a recognizable pattern onto the video data such

that the recognizable pattern appears on a viewing display when the video data is replayed.

The cited reference does not teach a method which includes providing a control signal that includes *a command to overlay a recognizable pattern* onto the video *data such that the recognizable pattern appears on a viewing display* when the video data is replayed. Rather, Park discloses a video security system that provides time stamps in a blanking interval to ensure the authenticity of the video signal. However, information located within a blanking interval is not visible in a video. Therefore, Park does not teach a control signal that includes *a command to overlay a recognizable pattern* onto the video *data such that the recognizable pattern appears on a viewing display* when the video data is replayed.

For the reasons stated above, claim 1 patentably distinguishes over the cited prior art, and the rejection of claim 1 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claim 1 is now in allowable condition.

Because claim 5 depends from and further limits claim 1, claim 5 is in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claim recites additional features which further patentably distinguish over the cited prior art.

Claims 7 and 9-11

Independent claim 7 has been amended to include all the limitations previously found in canceled dependent claim 9. Claim 7, as amended, recites an apparatus for authenticating video data including a processor that provides a control signal to a video data acquisition system. The processor receives an output signal from the data acquisition system including video data in response to providing the control signal. The processor verifies the authenticity of the video data from the data acquisition system by checking that the received output signal includes modifications according to the control signal. The data acquisition system, in response to receiving the control signal, overlays a recognizable

pattern onto the video data such that the recognizable pattern appears on a viewing display when the video data is replayed.

The cited reference does not teach an apparatus having a processor which provides a control signal that instructs the video data acquisition system to *overlay a recognizable pattern onto the video data such that the recognizable pattern appears on a viewing display* when the video data is replayed. Rather, as mentioned above in connection with claim 1, Park is directed to a video security system that provides time stamps in a blanking interval to ensure the authenticity of the video signal.

Accordingly, claim 19 distinguishes over the prior art for reasons similar to those presented above in connection with claim 1.

For the reasons stated above, claim 7 patentably distinguishes over the cited prior art, and the rejection of claim 7 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claim 7 is now in allowable condition.

Because claims 10-11 depend from and further limit claim 7, claims 10-11 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

Claims 14-15

Claim 14 recites an apparatus for maintaining video data, the apparatus having a video data processor that receives video data from a video data acquisition system. The video data is stored in a first memory storage device. The apparatus also has a hashing processor that generates a hash value based on a selected portion of the video data. The hash value is stored in the first memory storage device and a second memory storage device.

The cited reference does not teach an apparatus in which *video data* is *stored in a first memory storage device* and a *hash value* is *stored in the first*

memory storage device and a second memory storage device. Rather, Jones teaches a system for providing cryptographic security to a legacy system. The system of Jones creates a cryptographic hash 128, but stores it in only one storage location, together with the associated video content 11 on videotape 48. However, Jones does not teach an apparatus in which *video data* is *stored in a first memory storage device* and a *hash value* is *stored in the first memory storage device and a second memory storage device.*

For the reasons stated above, claim 14 patentably distinguishes over the cited prior art, and the rejection of claim 14 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claim 14 is in allowable condition.

Because claim 15 depends from and further limits claim 14, claim 15 is in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claim recites additional features which further patentably distinguish over the cited prior art.

Claims 12-13

Claim 12, as originally presented, recites limitations similar to those of claim 14. Accordingly, Applicants submit that claim 12 patentably distinguishes over the cite prior art for at least the same reasons as claim 14. Accordingly, the prior art rejection of claim 12 should be withdrawn, and claim 12 is in allowable condition.

Because claim 13 depends from and further limits claim 12, claim 13 is in allowable condition for at least the same reasons.

Claims 16-17 and 20

Independent claim 16 has been amended to include all the limitations previously found in canceled dependent claim 20. Claim 16, as amended, recites a method for generating an output signal from a video data acquisition system. The method includes (a) receiving a video signal that varies depending on

sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) implementing a recognition algorithm to identify objects associated with the sensed images, and (e) in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.

The cited references to do not teach or suggest, either alone or in combination, a method including (a) receiving a video signal that varies depending on sensed images, (b) encrypting the video signal using a first key, (c) encrypting the first key using a second key, (d) including at least the encrypted first key and encrypted video signal in the output signal, (d) *implementing a recognition algorithm to identify objects associated with the sensed images*, and (e) *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.* Peters teaches a technique for deterring theft of media recording devices in which an asymmetric key may be used to encrypt a symmetric key which was used to encrypt video data recorded by a media device. However, Peters does not teach *implementing a recognition algorithm to identify objects associated with the sensed images*, and *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.* The Office Action, on page 14, cites Chainer (Figs. 2-3, Col. 4, line 30 through Col. 6, line 17, and Col. 7, lines 52-61) as teaching that additional feature. However, the cited portion of Chainer does not teach *implementing a recognition algorithm to identify objects associated with the sensed images*, and *in response to recognizing an object, embedding encrypted data information identifying the recognized object in the output signal.* Rather, Chainer teaches using an RFID tag reader 103 or other measuring device 400 to identify an object, but not a *recognition algorithm to identify* an object from a sensed image. If the rejection of claim 16 is to be maintained, Applicants respectfully request that it be pointed out with particularity where the cited prior art teaches such a *recognition algorithm.*

For the reasons stated above, claim 16 patentably distinguishes over the cited prior art, and the rejection of claim 16 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claim 16 is now in allowable condition.

Because claim 17 depends from and further limits claim 16, claim 17 is in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claim recites additional features which further patentably distinguish over the cited prior art.

Claims 31-32 and 35

Claim 31 was amended to include all of the limitations of claim 35. Applicants submit that claim 31 now recites language similar to that of claim 16. Accordingly, Applicants submit that claim 31 patentably distinguishes over the cite prior art for at least the same reasons as claim 16. Accordingly, the prior art rejection of claim 31 should be withdrawn, and claim 31 is in allowable condition.

Because claim 32 depends from and further limits claim 31, claim 32 is in allowable condition for at least the same reasons.

Claim 37

Claim 37 was amended to include the limitations of claim 20 which included language similar to that recited in claim 16. Accordingly, Applicants submit that claim 37 patentably distinguishes over the cite prior art for reasons similar to those set forth above for claim 16. Accordingly, the prior art rejection of claim 37 should be withdrawn, and claim 37 is in allowable condition.

Claim 38

Claim 38 was amended to include the limitations of claim 20 which included language similar to that recited in claim 16. Accordingly, Applicants submit that claim 38 patentably distinguishes over the cite prior art for reasons

similar to those set forth above for claim 16. Accordingly, the prior art rejection of claim 38 should be withdrawn, and claim 38 is in allowable condition.

Claims 21-25

Independent claim 21 has been amended to include all the limitations previously found in canceled dependent claim 23. Claim 21, as amended, recites a method for maintaining video data. The method includes (a) providing an encryption key to a video data acquisition system, (b) encrypting at least a portion of an output signal generated by the video data acquisition system using the provided encryption key, (c) maintaining confidentiality of the provided encryption key so that recorded subjects of the video data acquisition system do not have access to the provided encryption key, knowledge of the provided encryption key being entrusted to an escrow agent, and (d) notifying the escrow agent to decrypt selected portions of the output signal previously stored in memory using the provided encryption key.

The cited reference does not teach a method which includes maintaining confidentiality of the provided encryption key so that recorded subjects of the video data acquisition system do not have access to the provided encryption key, knowledge of the provided encryption key being entrusted to an escrow agent, and *notifying the escrow agent to decrypt selected portions of the output signal* previously stored in memory using the provided encryption key. Rather, Peters teaches a technique for deterring theft of media recording devices by having the device encrypt recorded video so that an unauthorized user cannot access it properly. Peters also teaches that in order to aid a customer who has lost his or her key to a device, a manufacturer may provide a key escrow service to give a customer the key upon presentation of some proof of ownership of the device (Paragraph 0043). However, Peters does not teach *notifying the escrow agent to decrypt selected portions of the output signal* previously stored in memory using

the provided encryption key. Rather, Peters merely has the escrow agent provide a lost key to a customer.

For the reasons stated above, claim 21 patentably distinguishes over the cited prior art, and the rejection of claim 21 under 35 U.S.C. §102(e) should be withdrawn. Accordingly, claim 21 is now in allowable condition.

Because claims 22 and 24-25 depend from and further limit claim 21, claims 22 and 24-25 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recite additional features which further patentably distinguish over the cited prior art.

For example, claim 22 recites a method as in claim 21 further comprising *verifying an authenticity* of the output signal by checking that at least a portion of the output signal is encrypted with the provided key. However, Peters is directed to a technique for deterring theft of media recording devices by having the device encrypt recorded video so that an unauthorized user cannot access it properly. Peters does not teach *verifying an authenticity* of the output signal – rather it teaches verifying a particular user's right to access data and equipment. If the rejection of claim 2 is to be maintained, Applicant respectfully requests that it be pointed out with particularity where the cited prior art teaches *verifying an authenticity* of the output signal by checking that at least a portion of the output signal is encrypted with the provided key.

Claims 26-30

Claim 26 recites a method for generating an output signal from a video data acquisition system, the method including (a) receiving a video signal that varies depending on images detected by a video camera, (b) encrypting a selected portion of the video signal using a first encryption key, (c) receiving a sensor signal that varies depending on detection of objects in a vicinity of the data acquisition system, (d) encrypting a selected portion of the sensor signal

using a second encryption key, and (e) producing the output signal to include at least the encrypted video signal and the encrypted sensor signal.

The cited reference does not teach a method which includes *encrypting a selected portion of the video signal using a first encryption key* and *encrypting a selected portion of the sensor signal using a second encryption key*. Rather, Chainer discloses a system and method for authenticating an image of an object. A composite generator 105 combines the image and the sensed RFID results to encode the tag ID information together with a hash of the image (Col. 4, lines 37-48). This encoded data may be encrypted for further security (Col. 5, lines 43-54). Thus, a hash of an image from a camera 104 and sensed data may be combined and jointly encrypted using a single key, but nowhere does Chainer teach using two keys to separately encrypt *a selected portion of* a *video signal* and *a selected portion of* a *sensor signal*. Furthermore, this feature of claim 26 provides a special benefit not available from the system of Chainer: "The use of multiple encryption keys to encrypt different portions of the data in output signal 580 provides security and flexibility because decryption of output signal 580 is limited depending on which encryption keys are known to a user attempting decryption" (Specification, page 14, lines 11-14).

For the reasons stated above, claim 26 patentably distinguishes over the cited prior art, and the rejection of claim 26 under 35 U.S.C. §102(b) should be withdrawn. Accordingly, claim 26 is in allowable condition.

Because claims 27-30 depend from and further limits claim 26, claims 27-30 are in allowable condition for at least the same reasons. Additionally, it should be understood that the dependent claims recites additional features which further patentably distinguish over the cited prior art.

Claim 36

Claim 36 recites language similar to that recited in claim 26. Accordingly, Applicants submit that claim 36 patentably distinguishes over the cite prior art for

reasons similar to those set forth above for claim 26. Accordingly, the prior art rejection of claim 36 should be withdrawn, and claim 36 is in allowable condition.

Newly Added Claims

Claims 39-42 have been added and are believed to be in allowable condition. Claim 39 depends from claim 12. Claim 40 depends from claim 14. Claim 41 depends from claim 26. Claim 42 depends from claim 36. Support for claims 39-40 is provided within the Specification, for example, on page 8, line 24 through page 10, line 28. Support for claims 41-42 is provided within the Specification, for example, on page 17, lines 23-28. No new matter has been added.

Conclusion

In view of the foregoing remarks, this Application should be in condition for allowance. A Notice to this affect is respectfully requested. If the Examiner believes, after this Amendment, that the Application is not in condition for allowance, the Examiner is respectfully requested to call the Applicants' Representative at the number below.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this Amendment, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3661.

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-2900, in Westborough, Massachusetts.

Respectfully submitted,

David E. Huang, Esq.
Attorney for Applicants
Registration No.: 39,229
Bainwood, Huang & Associates, L.L.C.
Highpoint Center
2 Connector Road
Westborough, Massachusetts 01581
Telephone: (508) 616-2900
Facsimile: (508) 366-4688

Attorney Docket No.: 1004-120

Dated: January 26, 2007